

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	795	713/189.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:13
L2	282	713/166.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:13
L3	1168	713/168.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:17
L4	161	726/25.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:06
L5	1055	380/28.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:07
L6	459	380/37.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:08
L7	285	380/42.ccls. and @ad<"20030121"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:07
L8	3709	(L1 or L2 or L3 or L4 or L5 or L6 or L7)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:08

EAST Search History

L9	2590	(cipher\$3 or encrypt\$3 or encipher\$3 or cryptograph\$4) with (strength or weakness or provab\$6 or probab\$6 or value) with (evaluat\$3 or determin\$3 or measur\$3 or scal\$3 or factor\$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:18
L10	32829	(Feistel or CAST or MISTY\$2) same (cipher\$3 or encrypt\$3 or encipher\$3 or cryptograph\$4 or algorithm or function or equation)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:13
L11	3490443	(output or result or parameter or value) with (step\$3 or round or process or function\$3 or calculat\$3 or determin\$3 or condition)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:13
L12	948720	polynomial or algebraic or equation or algorithm	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:13
L13	28791	(cipher\$3 or encrypt\$3 or encipher\$3 or cryptograph\$4) with (strength or weakness or provab\$6 or probab\$6 or value or evaluat\$3 or determin\$3 or measur\$3 or scal\$3 or factor\$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:16
L14	4656	L10 and L11 and L12	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:17
L15	102	L14 and L8 and L13	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:18
L16	29	L14 and L8 and L9	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:20

EAST Search History

L17	2	"20050235342"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:18
L18	79	Tsunoo.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:18
L19	13	(cipher\$3 or encrypt\$3 or encipher\$3 or cryptograph\$4) and L18	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/22 15:19

Inventor Information for 10/762653

Inventor Name	City	State/Country
TANAKA, HIDE MA	KOGANEI	JAPAN
KANEKO, TOSHINOBU	NODA	JAPAN
HATANO, YASUO	NODA	JAPAN

[Appln Info](#)[Contents](#)[Petition Info](#)[Atty/Agent Info](#)[Continuity/Reexam](#)[Foreign Data](#)**Inventor**

Search Another: Application#

or Patent#

PCT / /

or PG PUBS #

Attorney Docket #

Bar Code #

To go back use Back button on your browser toolbar.

Back to [PALM](#) | [ASSIGNMENT](#) | [OASIS](#) | [Home page](#)


☐ Search Results

BROWSE

SEARCH

IEEE XPLORE GUIDE

SUPPORT

Results for "(((cast and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)"

Your search matched 7 of 1589326 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.

e-mail printer friendly

» Search Options

[View Session History](#)

[New Search](#)

Modify Search

(((cast and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)

Search

☐ Check to search only within this results set

Display Format: ☒ Citation ☐ Citation & Abstract

» Key



Indicates full text access

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

view selected items

[Select All](#) [Deselect All](#)

- ☐ **1. The analysis of a new class of unbalanced CAST ciphers**
 Zhu, X.; Heys, H.M.;
[Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on](#)
 Volume 1, 25-28 May 1997 Page(s):326 - 329 vol.1
 Digital Object Identifier 10.1109/CCECE.1997.614855
[Abstract](#) | Full Text: [PDF\(396 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ **2. Information leakage of Feistel ciphers**
 Heys, H.M.;
[Information Theory, IEEE Transactions on](#)
 Volume 47, Issue 1, Jan. 2001 Page(s):23 - 35
 Digital Object Identifier 10.1109/18.904500
[Abstract](#) | Full Text: [PDF\(316 KB\)](#) IEEE JNL
[Rights and Permissions](#)
- ☐ **3. An analysis of the CAST-256 cipher**
 Adams, C.; Heys, H.M.; Tavares, S.E.; Wiener, M.;
[Electrical and Computer Engineering, 1999 IEEE Canadian Conference on](#)
 Volume 1, 9-12 May 1999 Page(s):361 - 366 vol.1
 Digital Object Identifier 10.1109/CCECE.1999.807225
[Abstract](#) | Full Text: [PDF\(420 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ **4. Enhancing the security of block ciphers with the aid of parallel substitution box construction**
 Nastou, P.; Stamatiou, Y.C.;
[Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on](#)
 2-5 July 2002 Page(s):29 - 34
 Digital Object Identifier 10.1109/ICDCSW.2002.1030744
[Abstract](#) | Full Text: [PDF\(339 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ **5. The FPGA implementation of the RC6 and CAST-256 encryption algorithms**
 Riaz, M.; Heys, H.M.;
[Electrical and Computer Engineering, 1999 IEEE Canadian Conference on](#)
 Volume 1, 9-12 May 1999 Page(s):367 - 372 vol.1
 Digital Object Identifier 10.1109/CCECE.1999.807226
[Abstract](#) | Full Text: [PDF\(464 KB\)](#) IEEE CNF
[Rights and Permissions](#)

- ☐ **6. On the security of the CAST encryption algorithm**
Heys, H.M.; Tavares, E.;
[Electrical and Computer Engineering, 1994. Conference Proceedings. 1994 Canadian Conference on](#)
25-28 Sept. 1994 Page(s):332 - 335 vol.1
Digital Object Identifier 10.1109/CCECE.1994.405756
[Abstract](#) | [Full Text: PDF\(260 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ **7. Dynamically modifiable ciphers using a reconfigurable CAST-128 based algorithm on AMTEL's FPSLIC reconfigurable FPGA architecture**
Nastou, P.E.; Stamatou, Y.C.;
[Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, Abstracts and CD-ROM](#)
15-19 April 2002 Page(s):157 - 163
[Abstract](#) | [Full Text: PDF\(379 KB\)](#) IEEE CNF
[Rights and Permissions](#)



Welcome United States Patent and Trademark Office

☐ Search Results[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)[SUPPORT](#)

Results for "(((feistel and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)"

Your search matched 6 of 1589326 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

e-mail
 printer friendly

» Search Options

[View Session History](#)[New Search](#)

Modify Search

(((feistel and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)

[Search](#) >☐ Check to search only within this results setDisplay Format: ☒ Citation ☐ Citation & Abstract[view selected items](#)[Select All](#) [Deselect All](#)

- IEEE JNL IEEE Journal or Magazine
- IET JNL IET Journal or Magazine
- IEEE CNF IEEE Conference Proceeding
- IET CNF IET Conference Proceeding
- IEEE STD IEEE Standard

- ☐ 1. **Information leakage of Feistel ciphers**
Heys, H.M.;
[Information Theory, IEEE Transactions on](#)
Volume 47, Issue 1, Jan. 2001 Page(s):23 - 35
Digital Object Identifier 10.1109/18.904500
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(316 KB\)](#) IEEE JNL
[Rights and Permissions](#)
- ☐ 2. **The SHADE cipher: an efficient hash-function-based Feistel network**
Adams, C.;
[Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on](#)
Volume 1, 25-28 May 1997 Page(s):338 - 342 vol.1
Digital Object Identifier 10.1109/CCECE.1997.614858
[AbstractPlus](#) | Full Text: [PDF\(480 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ 3. **Application of multilayer perceptron networks in symmetric block ciphers**
Liew Pol Yee; De Silva, L.C.;
[Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on](#)
Volume 2, 12-17 May 2002 Page(s):1455 - 1458
Digital Object Identifier 10.1109/IJCNN.2002.1007731
[AbstractPlus](#) | Full Text: [PDF\(396 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ 4. **On the hypothesis of stochastic equivalence for Feistel ciphers**
Canteaut, A.;
[Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on](#)
16-21 Aug. 1998 Page(s):81
Digital Object Identifier 10.1109/ISIT.1998.708666
[AbstractPlus](#) | Full Text: [PDF\(88 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐ 5. **Some cryptographic techniques for machine-to-machine data communications**
Feistel, H.; Notz, W.A.; Smith, J.L.;
[Proceedings of the IEEE](#)
Volume 63, Issue 11, Nov. 1975 Page(s):1545 - 1554
[AbstractPlus](#) | Full Text: [PDF\(1116 KB\)](#) IEEE JNL
[Rights and Permissions](#)
- ☐ 6. **Security issues based on chaotic systems**
Filippini, A.; Bergamo, P.; Mazzini, G.;

Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE
Volume 1, 17-21 Nov. 2002 Page(s):148 - 152 vol.1

AbstractPlus | Full Text: PDF(359 KB) IEEE CNF
Rights and Permissions

Indexed by
 Inspec*

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved



Welcome United States Patent and Trademark Office

Search Results

BROWSESEARCHIEEE XPLORE GUIDESUPPORT

Results for "(((misty1 and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)"

Your search matched 2 of 1589326 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

e-mail printer friendly

» Search Options

[View Session History](#)
[New Search](#)

Modify Search

(((misty1 and cipher)<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2003)

Search

☐ Check to search only within this results set

Display Format: ☒ Citation ☐ Citation & Abstract

» Key

- IEEE JNL IEEE Journal or Magazine
- IET JNL IET Journal or Magazine
- IEEE CNF IEEE Conference Proceeding
- IET CNF IET Conference Proceeding
- IEEE STD IEEE Standard

view selected items

Select AllDeselect All

- ☐
1. A time and area efficient hardware implementation of the MISTY1 block cipher

Kitsos, P.; Koufopavlou, O.;
[Circuits and Systems, 2003. MWSCAS '03. Proceedings of the 46th IEEE International Midwest Symposium on](#)
Volume 2, 27-30 Dec. 2003 Page(s):794 - 797 Vol. 2
Digital Object Identifier 10.1109/MWSCAS.2003.1562406

[AbstractPlus](#) | Full Text: [PDF\(640 KB\)](#) IEEE CNF
[Rights and Permissions](#)
- ☐
2. Efficient FPGA implementation of block cipher MISTY1

Rouvroy, G.; Standaert, F.-X.; Quisquater, J.-J.; Legat, J.-D.;
[Parallel and Distributed Processing Symposium, 2003. Proceedings. International](#)
22-26 April 2003 Page(s):7 pp.
Digital Object Identifier 10.1109/IPDPS.2003.1213343

[AbstractPlus](#) | Full Text: [PDF\(339 KB\)](#) IEEE CNF
[Rights and Permissions](#)

